Scishare: A Secure P2P Information Sharing Tool

Karlo Berket,

Abdelilah Essiari, Artur Muratas

Lawrence Berkeley National Lab

SDSC - Feb. 17, 2005

Outline

- Requirements
- System architecture
- Meeting the security requirements
  - PKI-based peer-to-peer security
- Software implementation

Requirements

- Share local data
  - Keeps data in owner's hands
  - Allows faster access to updates
    - Don't have to wait for transfer to repository
  - Central repository is no longer a requirement
    - Better scalability and fault-tolerance of system
    - Easier to consolidate existing information stores
  - Easy-to-use fine-grained access control interface is a must

Requirements

- Allow for extensible search
  - Search important feature for information systems
    - Where would the web be without search engines
  - Extensibility important
    - Goal is not to create a data representation standard
    - Allow different disciplines/applications to use the query language and data representation they are familiar with
    - Don’t require translation of existing information to use the system

Requirements

- Security
  - Confidentiality and integrity of communication
  - Fine-grained access control to resources
- Support ad hoc collaborations
  - Meetings at conferences
  - Requires flexible security model
    - Quick and easy startup
    - Trust building

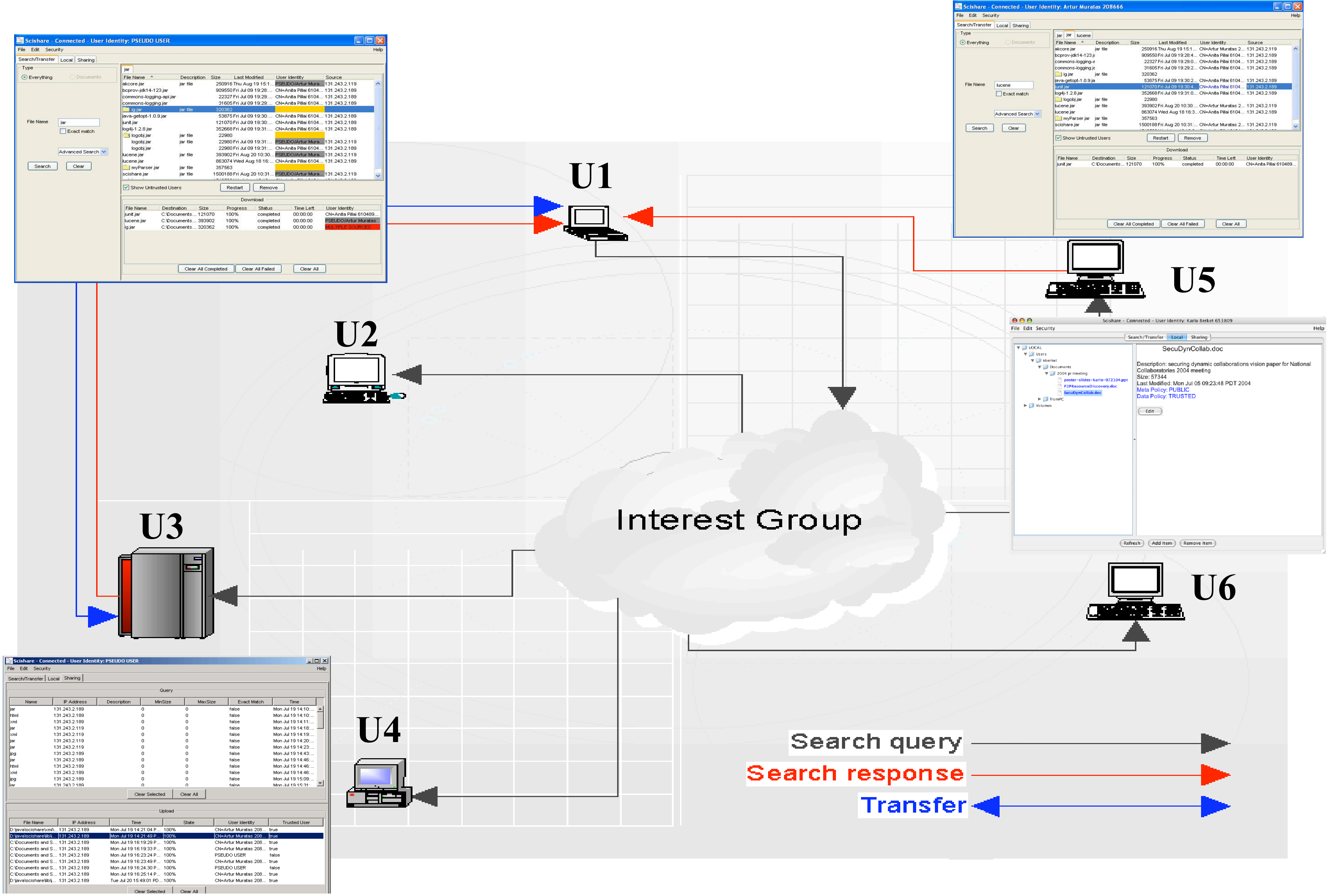
Requirements

- Reach a wide community
  - Run on many OS and architectures
- Do it all in short time with limited personnel
  - Need to use existing technology whenever possible

Outline

- Requirements
- System architecture
- Meeting the security requirements
  - PKI-based peer-to-peer security
- Software implementation

Scishare Architecture



Scishare - Connected - User Identity: PSEUDO USER

○ Everything ○ Documents

File Name: jar

□ Exact match

File Name ^	Description	Size	Last Modified	User Identity	Source
akcore.jar	jar file	250916	Thu Aug 19 15:1...	PSEUDO/Artur Mura...	131.243.2.119
bcprov-jdk14-123.jar		909550	Fri Jul 09 19:28:...	CN=Anita Pillai 6104...	131.243.2.189
commons-logging-api.jar		22327	Fri Jul 09 19:29:...	CN=Anita Pillai 6104...	131.243.2.189
commons-logging.jar		31605	Fri Jul 09 19:29:...	CN=Anita Pillai 6104...	131.243.2.189
ig.jar	jar file	320362			
java-getopt-1.0.9.jar		53875	Fri Jul 09 19:30:...	CN=Anita Pillai 6104...	131.243.2.189
junit.jar		121070	Fri Jul 09 19:30:...	CN=Anita Pillai 6104...	131.243.2.189
log4j-1.2.8.jar		352668	Fri Jul 09 19:31:...	CN=Anita Pillai 6104...	131.243.2.189
logobj.jar	jar file	22980			
logobj.jar	jar file	22980	Fri Jul 09 19:31:...	PSEUDO/Artur Mura...	131.243.2.119
logobj.jar		22980	Fri Jul 09 19:31:...	CN=Anita Pillai 6104...	131.243.2.189
lucene.jar	jar file	393902	Fri Aug 20 10:30...	PSEUDO/Artur Mura...	131.243.2.119
lucene.jar		863074	Wed Aug 18 16:...	CN=Anita Pillai 6104...	131.243.2.189
myParser.jar	jar file	357563			
scishare.jar	jar file	1500188	Fri Aug 20 10:31...	PSEUDO/Artur Mura...	131.243.2.119

☑ Show Untrusted Users

Download

File Name	Destination	Size	Progress	Status	Time Left	User Identity
junit.jar	C:\Documents...	121070	100%	completed	00:00:00	CN=Anita Pillai 610489...
lucene.jar	C:\Documents...	393902	100%	completed	00:00:00	PSEUDO/Artur Muratas
ig.jar	C:\Documents...	320362	100%	completed	00:00:00	MULTIPLE SOURCES

Scishare - Connected - User Identity: Artur Muratas 208666

○ Everything ○ Documents

File Name: lucene

□ Exact match

File Name ^	Description	Size	Last Modified	User Identity	Source
akcore.jar	jar file	250916	Thu Aug 19 15:1...	CN=Artur Muratas 2...	131.243.2.119
bcprov-jdk14-123.ja		909550	Fri Jul 09 19:28:4...	CN=Anita Pillai 6104...	131.243.2.189
commons-logging-a		22327	Fri Jul 09 19:29:0...	CN=Anita Pillai 6104...	131.243.2.189
commons-logging.ja		31605	Fri Jul 09 19:29:2...	CN=Anita Pillai 6104...	131.243.2.189
ig.jar	jar file	320362			
java-getopt-1.0.9.ja		53875	Fri Jul 09 19:30:2...	CN=Anita Pillai 6104...	131.243.2.189
junit.jar		121070	Fri Jul 09 19:30:4...	CN=Anita Pillai 6104...	131.243.2.189
log4j-1.2.8.jar		352668	Fri Jul 09 19:31:0...	CN=Anita Pillai 6104...	131.243.2.189
logobj.jar	jar file	22980			
lucene.jar	jar file	393902	Fri Aug 20 10:30:...	CN=Artur Muratas 2...	131.243.2.119
lucene.jar		863074	Wed Aug 18 16:3...	CN=Anita Pillai 6104...	131.243.2.189
myParser.jar	jar file	357563			
scishare.jar	jar file	1500188	Fri Aug 20 10:31:...	CN=Artur Muratas 2...	131.243.2.119

☑ Show Untrusted Users

Download

File Name	Destination	Size	Progress	Status	Time Left	User Identity
junit.jar	C:\Documents...	121070	100%	completed	00:00:00	CN=Anita Pillai 610489...

Scishare – Connected – User Identity: Karlo Berket 653809

SecuDynCollab.doc

Description: securing dynamic collaborations vision paper for National Collaboratories 2004 meeting
Size: 57344
Last Modified: Mon Jul 05 09:23:48 PDT 2004
Meta Policy: PUBLIC
Data Policy: TRUSTED

Scishare - Connected - User Identity: PSEUDO USER

Query

Name	IP Address	Description	MinSize	MaxSize	Exact Match	Time
jar	131.243.2.189		0	0	false	Mon Jul 19 14:10:...
html	131.243.2.189		0	0	false	Mon Jul 19 14:10:...
xml	131.243.2.189		0	0	false	Mon Jul 19 14:11:...
jar	131.243.2.119		0	0	false	Mon Jul 19 14:18:...
xml	131.243.2.119		0	0	false	Mon Jul 19 14:19:...
jar	131.243.2.119		0	0	false	Mon Jul 19 14:20:...
jar	131.243.2.119		0	0	false	Mon Jul 19 14:23:...
jpg	131.243.2.189		0	0	false	Mon Jul 19 14:43:...
jar	131.243.2.189		0	0	false	Mon Jul 19 14:46:...
html	131.243.2.189		0	0	false	Mon Jul 19 14:46:...
xml	131.243.2.189		0	0	false	Mon Jul 19 14:46:...
jpg	131.243.2.189		0	0	false	Mon Jul 19 15:09:...
jar	131.243.2.189		0	0	false	Mon Jul 19 15:31:

Upload

File Name	IP Address	Time	State	User Identity	Trusted User
D:\java\scishare\xml\...	131.243.2.189	Mon Jul 19 14:21:04 P...	100%	CN=Artur Muratas 208...	true
D:\java\scishare\lib\i...	131.243.2.189	Mon Jul 19 14:21:49 P...	100%	CN=Artur Muratas 208...	true
C:\Documents and S...	131.243.2.189	Mon Jul 19 16:19:29 P...	100%	CN=Artur Muratas 208...	true
C:\Documents and S...	131.243.2.189	Mon Jul 19 16:19:33 P...	100%	CN=Artur Muratas 208...	true
C:\Documents and S...	131.243.2.189	Mon Jul 19 16:23:24 P...	100%	PSEUDO USER	false
C:\Documents and S...	131.243.2.189	Mon Jul 19 16:23:49 P...	100%	CN=Artur Muratas 208...	true
C:\Documents and S...	131.243.2.189	Mon Jul 19 16:24:30 P...	100%	PSEUDO USER	false
C:\Documents and S...	131.243.2.189	Mon Jul 19 16:25:14 P...	100%	CN=Artur Muratas 208...	true
D:\java\scishare\lib\j...	131.243.2.189	Tue Jul 20 15:49:01 PD...	100%	CN=Artur Muratas 208...	true

Outline

- Requirements
- System architecture
- Meeting the security requirements
  - PKI-based peer-to-peer security
- Software implementation

Security Goals

- Confidentiality and integrity of communication
- Fine-grained access control to resources
- Support ad hoc collaborations
- Assumption
  - X.509 identity certificates

Approach

- Use Public Key Infrastructure (PKI)
  - X509 certification/online CAs
  - Flexible Trust Models
  - Reduces Key Management issues
- Use existing PKI-based security technologies
  - Modifications are external
  - Reduce the risk of introducing security holes

Traditional Security Model

- Authorized users are predefined
  - In or out (of system)
  - Harder to meet ‘new people’ online in a collaboration
- Policies are managed by third party entities (administrators)
  - Valid in many use cases
  - Hard to start a spontaneous collaboration
    - Setup takes time
  - Hard to invite a person to an established collaboration
    - Must contact resource administrators
- Security becomes a nuisance
  - Users may resort to insecure solutions

A Flexible Security Model

- Partition the collaboration into two types of **secure** components:
  - Public
    - Capture users' identities
    - Gradual trust in the collaboration
    - Turn off public components => traditional model
  - Protected
    - Authorized users only
    - Give invitation/escort powers to some of these users
- Example of components:
    - Communication channels, online instruments, chat rooms, shared spaces, files, …

Components in scishare

- Unicast channels
  - Managed by the users participating in the communication
- Multicast channel
  - Managed by 'Third-Party administrators'
- Files and metadata
  - Managed by individual users

Securing Unicast

- Secure communication channel (SSL)
  - Confidentiality
  - Integrity
  - Authentication
    - Typically only server presents X509 certificate
    - Require both parties to present X509 certificate (mutual authentication)
      - Every user needs a certificate

Securing Unicast

- Provide users with pseudo (self-signed) X509 certificates if they don't have any
- Custom trust manager
  - Accepts any valid chain
  - Marks users as trusted if user and chain verify
  - Remember un-trusted users
    - Can later authorize un-trusted users based on experience
- A single channel can handle both protected and public traffic
  - Simplifies development

Securing Multicast

- Need a secure group communication channel with properties similar to SSL:
  - – implements an authenticated and encrypted group channel
  - – enables group members to establish a session key
  - – certificate-based access control

Securing Multicast

- Public group communication channel
  - Every user can join
- Protected group communication channel
  - Fine-grained access control
    - Join, invite, escort
    - Capabilities
      - Short lived, signed by the enforcers
    - Invitations/Escorts
      - Short lived, signed by authorized users
- A single communication channel
  - A protected channel over a public one (sub-group)

Securing Data and Metadata

- Provide a simple high level interface to users
  - Manage policies
  - Manage groups
- Authorization engine is used underneath (e.g. Akenti)
  - Distributed groups
  - User revocation
  - Future complex expressions
    - Time of day, …

Read More About It

K. Berket, A.Essiari and A. Muratas

PKI-Based Security for Peer-to-Peer Information Sharing

Proceedings of the Fourth IEEE International Conference on Peer-to-Peer Computing, Zurich, Switzerland, Aug. 25-27, 2004.

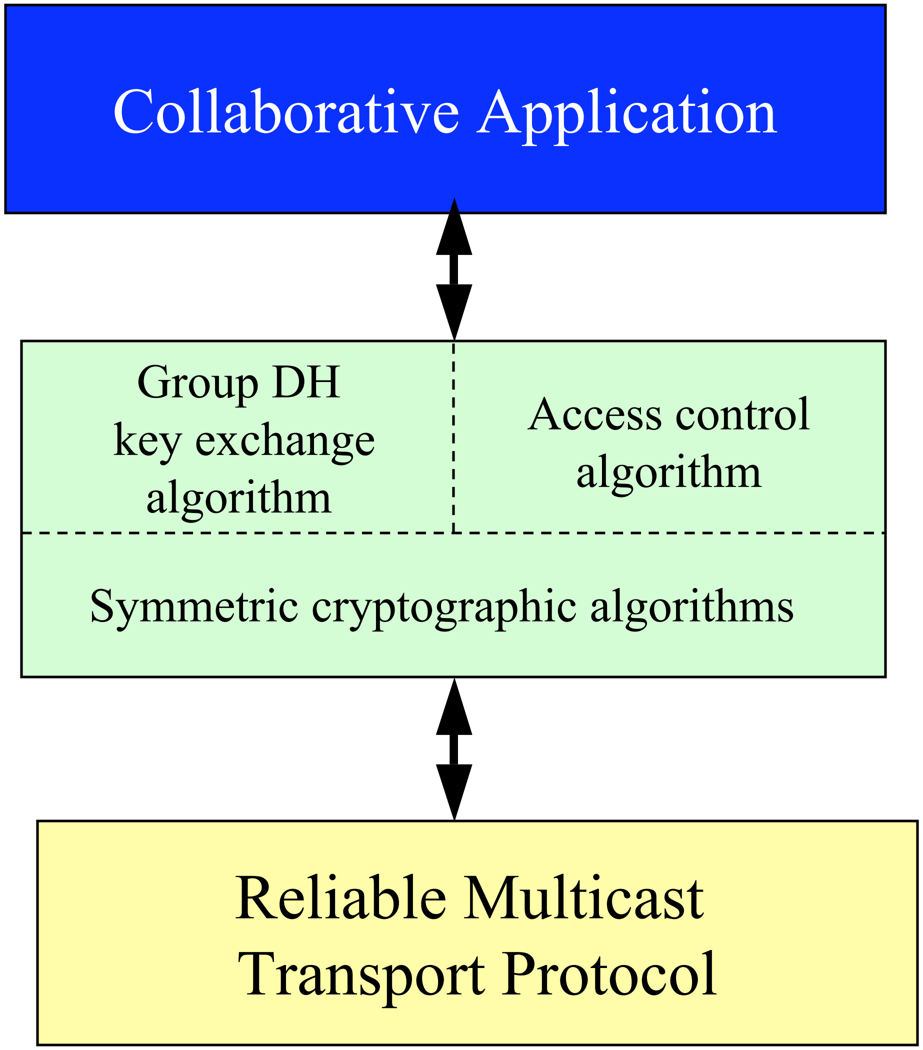
Outline

- Requirements
- System architecture
- Meeting the security requirements
  - PKI-based peer-to-peer security
- Software implementation

Build on Existing Tools

- XML messaging
  - JAXB to generate code from schema
- Securing the group communication channel
  - Secure Group Layer (SGL)
  - InterGroup
- Authorization engine
  - Akenti

Security at the Multicast-Transport Layer


Collaborative Application
Group DH key exchange algorithm
Access control algorithm
Symmetric cryptographic algorithms
Reliable Multicast Transport Protocol

Secure Group Layer (SGL)

The Reliable Multicast Transport Layer

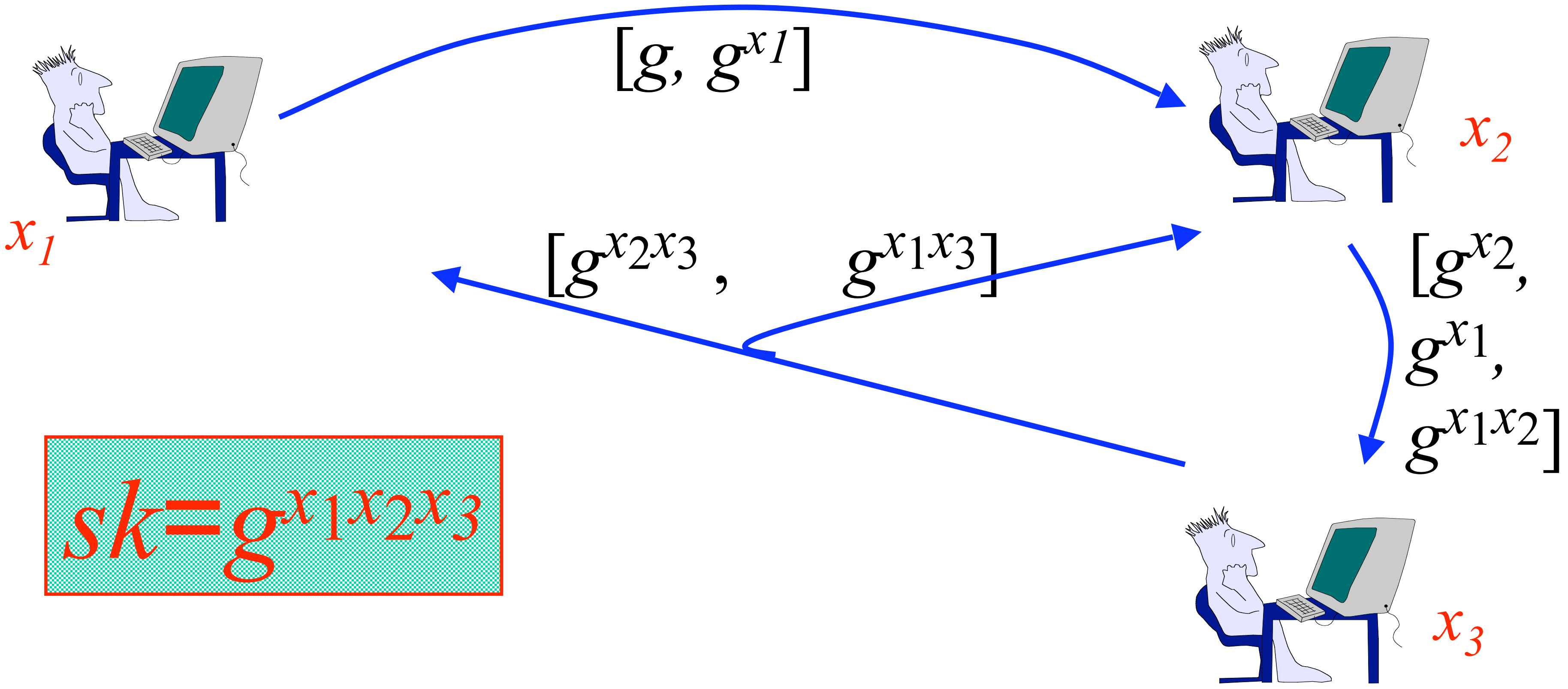
- Provide SGL with reliable and ordered delivery of messages
  - data messages are delivered in order - FIFO, partial, and total - at each member of the group
- Provide SGL with membership notifications
  - membership changes delivered in order with respect to data messages
- Several systems provide a reliable multicast layer
  - e.g., Totem and InterGroup

The Secure Group Layer

- Symmetric crypto algorithms
  - implement an authenticated and encrypted channel
- A group key-exchange cryptographic primitive enables group members to establish a session key
- A certificate-based access control mechanism makes sure that only the legitimate parties have access to the session key
  - off-line (does not participate in key exchange)

Group Key-Exchange

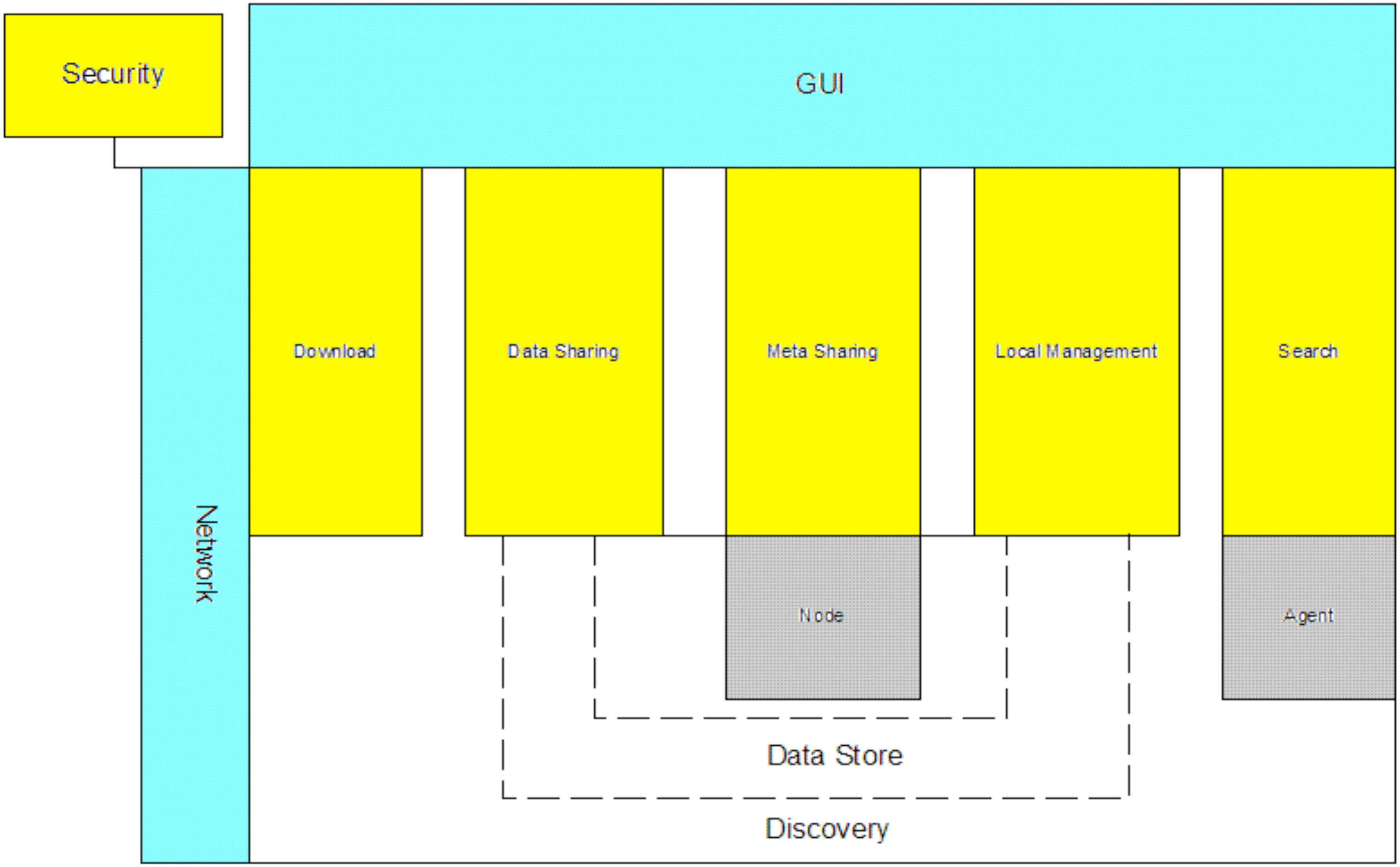
- Up-flow: U_i raises received values to the power of x_i and forwards to U_{i+1}
- Down-flow: U_n processes the last up-flow and broadcasts


$[g, g^{x_1}]$
x_1
x_2
$[g^{x_2 x_3}, \quad g^{x_1 x_3}]$
$[g^{x_2}, g^{x_1}, g^{x_1 x_2}]$
x_3
$sk = g^{x_1 x_2 x_3}$

Akenti Distributed Authorization

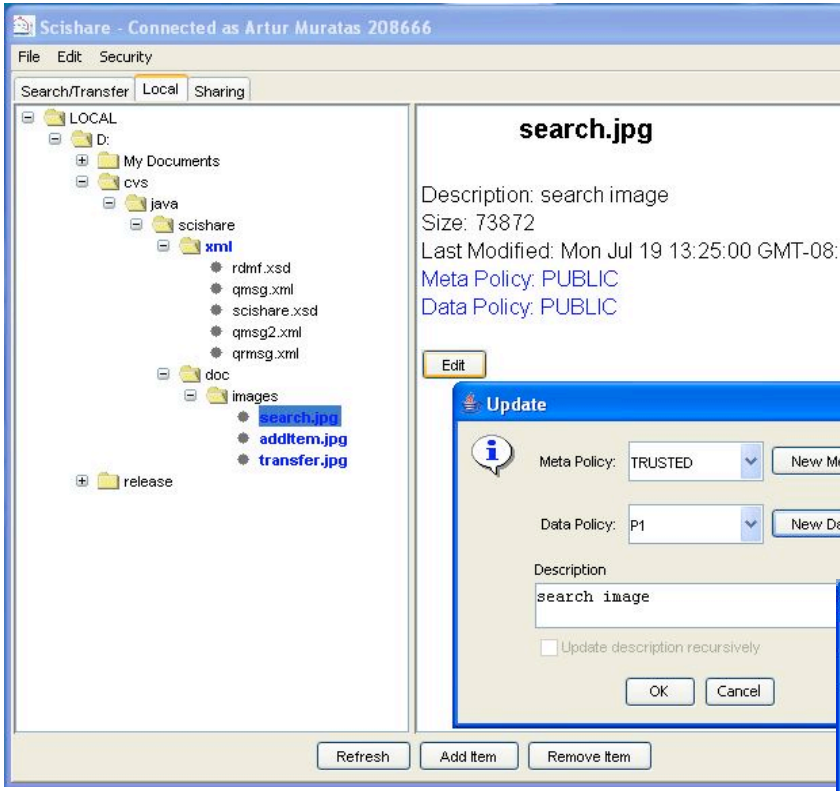
- Target widely distributed environments
  - Resources (instruments, executables, …)
  - Principals:
    - Resource owners (stakeholders)
    - User-Attribute Issuers
    - Users
- Collaborative/Grid environments that could span many autonomous/dispersed organizations.
- Provide a flexible and secure way for stakeholders to remotely and independently define authorization policy and allow fine-grained access control.

Software Architecture



Local

- Add/remove files in DB
- Synchronize DB with file system
- Map different policies to metadata and data



```
LOCAL
  D:
    My Documents
    cvs
      java
        scishare
          xml
            rdmf.xsd
            qmsg.xml
            scishare.xsd
            qmsg2.xml
            qrmsg.xml
          doc
            images
              search.jpg
              addItem.jpg
              transfer.jpg
    release
```

search.jpg

Description: search image
Size: 73872
Last Modified: Mon Jul 19 13:25:00 GMT-08:00 2004
Meta Policy: PUBLIC
Data Policy: PUBLIC

Meta Policy: TRUSTED

Data Policy: P1

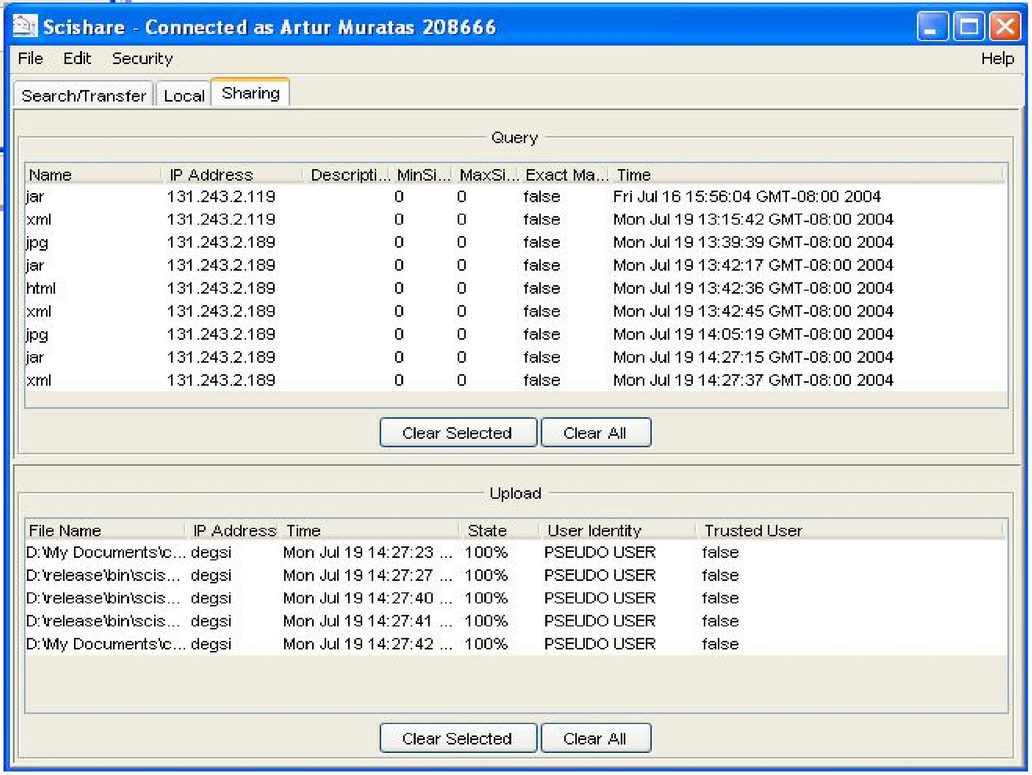
Description

search image

☐ Update description recursively

Sharing

- View incoming queries
- View file uploads



Query

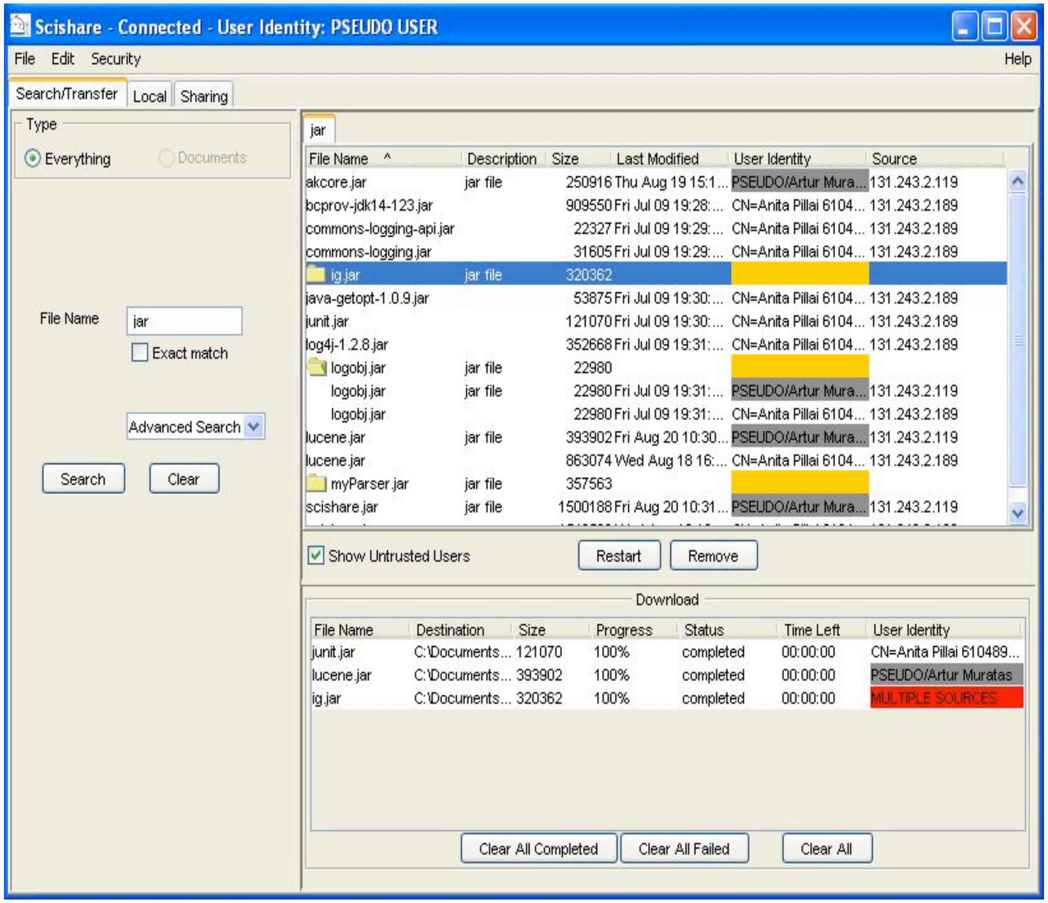
Name	IP Address	Descripti...	MinSi...	MaxSi...	Exact Ma...	Time
jar	131.243.2.119		0	0	false	Fri Jul 16 15:56:04 GMT-08:00 2004
xml	131.243.2.119		0	0	false	Mon Jul 19 13:15:42 GMT-08:00 2004
jpg	131.243.2.189		0	0	false	Mon Jul 19 13:39:39 GMT-08:00 2004
jar	131.243.2.189		0	0	false	Mon Jul 19 13:42:17 GMT-08:00 2004
html	131.243.2.189		0	0	false	Mon Jul 19 13:42:36 GMT-08:00 2004
xml	131.243.2.189		0	0	false	Mon Jul 19 13:42:45 GMT-08:00 2004
jpg	131.243.2.189		0	0	false	Mon Jul 19 14:05:19 GMT-08:00 2004
jar	131.243.2.189		0	0	false	Mon Jul 19 14:27:15 GMT-08:00 2004
xml	131.243.2.189		0	0	false	Mon Jul 19 14:27:37 GMT-08:00 2004

Upload

File Name	IP Address	Time	State	User Identity	Trusted User
D:\My Documents\c...	degsi	Mon Jul 19 14:27:23 ...	100%	PSEUDO USER	false
D:\release\bin\scis...	degsi	Mon Jul 19 14:27:27 ...	100%	PSEUDO USER	false
D:\release\bin\scis...	degsi	Mon Jul 19 14:27:40 ...	100%	PSEUDO USER	false
D:\release\bin\scis...	degsi	Mon Jul 19 14:27:41 ...	100%	PSEUDO USER	false
D:\My Documents\c...	degsi	Mon Jul 19 14:27:42 ...	100%	PSEUDO USER	false

Search - Transfer

- Create basic and advanced queries
- Start a search
- Group search results based on the same hash
- Display the origin of the metadata and its trustworthiness
- Allow user to download portions of a file in parallel
- Display the origin of the file and its trustworthiness



● Everything

File Name: jar

□ Exact match

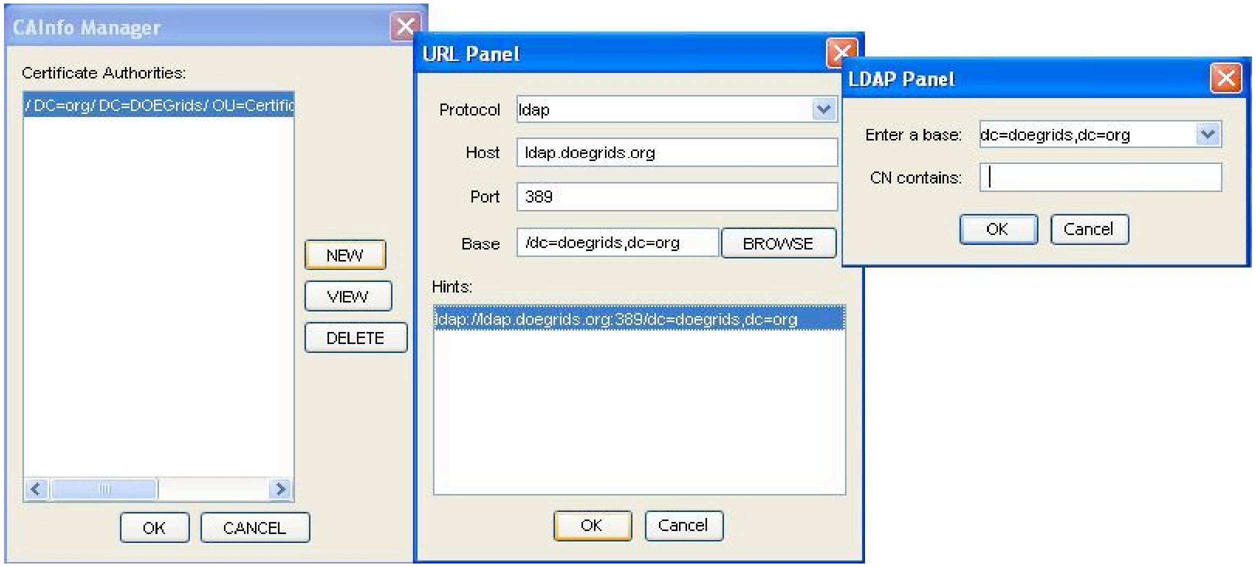
Advanced Search

File Name ^	Description	Size	Last Modified	User Identity	Source
akcore.jar	jar file	250916	Thu Aug 19 15:1...	PSEUDO/Artur Mura...	131.243.2.119
bcprov-jdk14-123.jar		909550	Fri Jul 09 19:28:...	CN=Anita Pillai 6104...	131.243.2.189
commons-logging-api.jar		22327	Fri Jul 09 19:29:...	CN=Anita Pillai 6104...	131.243.2.189
commons-logging.jar		31605	Fri Jul 09 19:29:...	CN=Anita Pillai 6104...	131.243.2.189
ig.jar	jar file	320362			
java-getopt-1.0.9.jar		53875	Fri Jul 09 19:30:...	CN=Anita Pillai 6104...	131.243.2.189
junit.jar		121070	Fri Jul 09 19:30:...	CN=Anita Pillai 6104...	131.243.2.189
log4j-1.2.8.jar		352668	Fri Jul 09 19:31:...	CN=Anita Pillai 6104...	131.243.2.189
logobj.jar	jar file	22980			
logobj.jar	jar file	22980	Fri Jul 09 19:31:...	PSEUDO/Artur Mura...	131.243.2.119
logobj.jar		22980	Fri Jul 09 19:31:...	CN=Anita Pillai 6104...	131.243.2.189
lucene.jar	jar file	393902	Fri Aug 20 10:30...	PSEUDO/Artur Mura...	131.243.2.119
lucene.jar		863074	Wed Aug 18 16:...	CN=Anita Pillai 6104...	131.243.2.189
myParser.jar	jar file	357563			
scishare.jar	jar file	1500188	Fri Aug 20 10:31...	PSEUDO/Artur Mura...	131.243.2.119

☑ Show Untrusted Users

File Name	Destination	Size	Progress	Status	Time Left	User Identity
junit.jar	C:\Documents...	121070	100%	completed	00:00:00	CN=Anita Pillai 610489...
lucene.jar	C:\Documents...	393902	100%	completed	00:00:00	PSEUDO/Artur Muratas
ig.jar	C:\Documents...	320362	100%	completed	00:00:00	MULTIPLE SOURCES

Manage CAs



Certificate Authorities: / DC=org/ DC=DOEGrids/ OU=Certific

Protocol: ldap

Host: ldap.doegrids.org

Port: 389

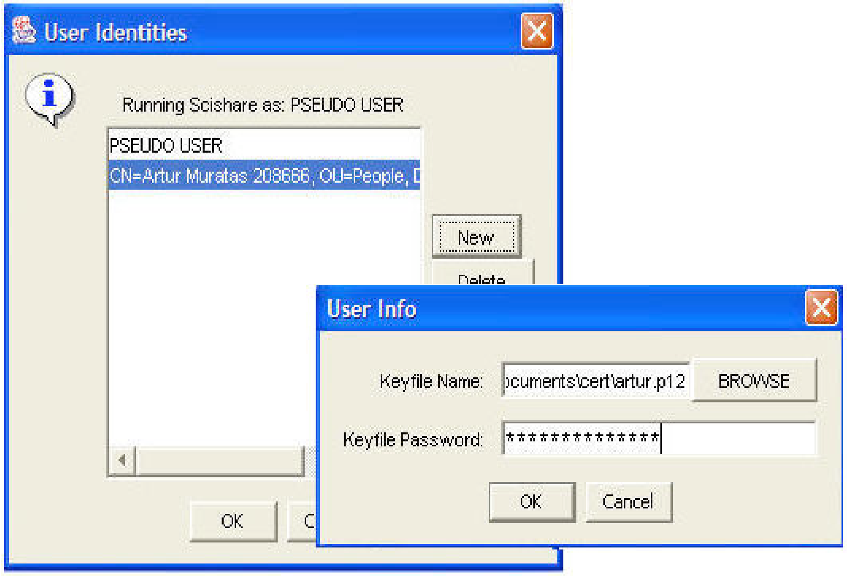
Base: /dc=doegrids,dc=org

Hints: ldap://ldap.doegrids.org:389/dc=doegrids,dc=org

Enter a base: dc=doegrids,dc=org

CN contains:

Manage User Identity



Running Scishare as: PSEUDO USER

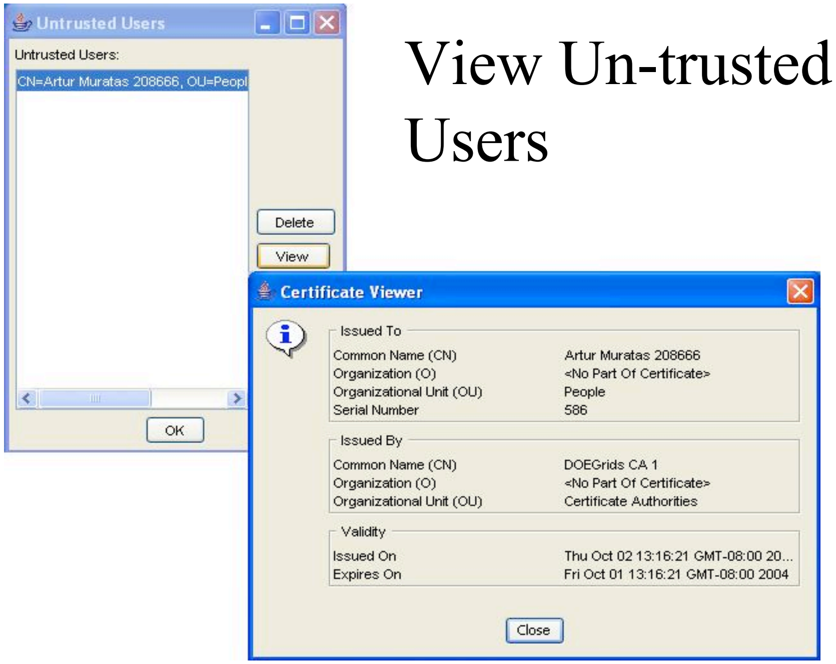
PSEUDO USER

CN=Artur Muratas 208666, OU=People, D

Keyfile Name: ocuments\cert\artur.p12

Keyfile Password: **************

View Un-trusted Users



Untrusted Users: CN=Artur Muratas 208666, OU=Peopl

Issued To

Common Name (CN)	Artur Muratas 208666
Organization (O)	<No Part Of Certificate>
Organizational Unit (OU)	People
Serial Number	586

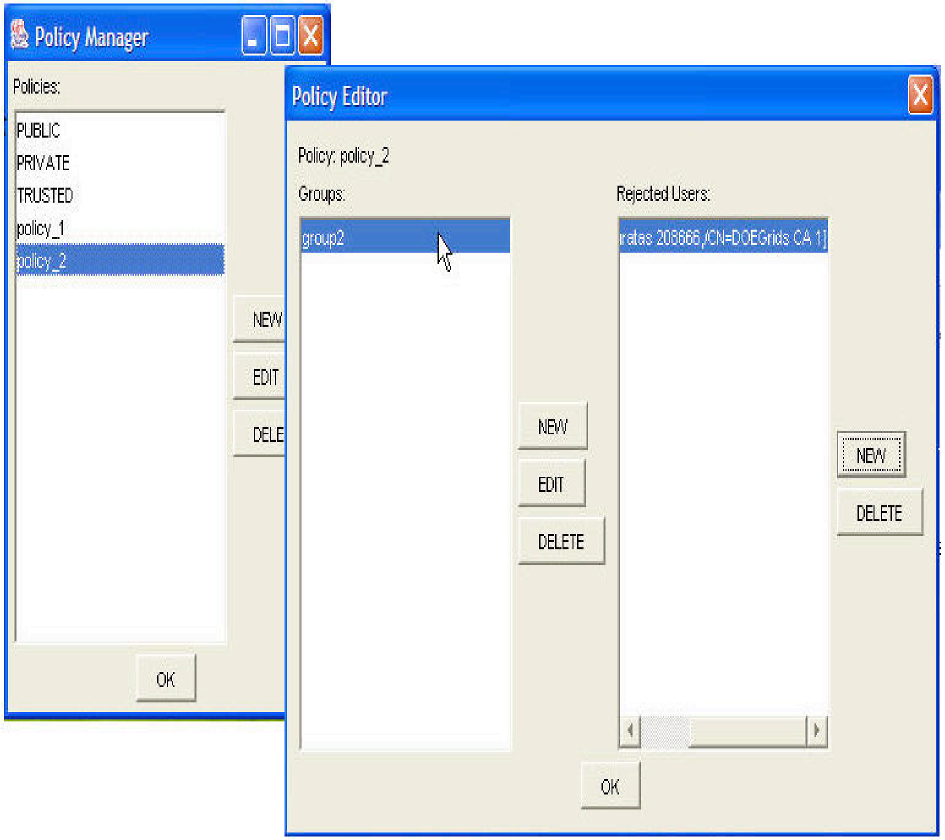
Issued By

Common Name (CN)	DOEGrids CA 1
Organization (O)	<No Part Of Certificate>
Organizational Unit (OU)	Certificate Authorities

Validity

Issued On	Thu Oct 02 13:16:21 GMT-08:00 20...
Expires On	Fri Oct 01 13:16:21 GMT-08:00 2004

Manage Policies



Policies:

PUBLIC
PRIVATE
TRUSTED
policy_1
policy_2

Policy: policy_2

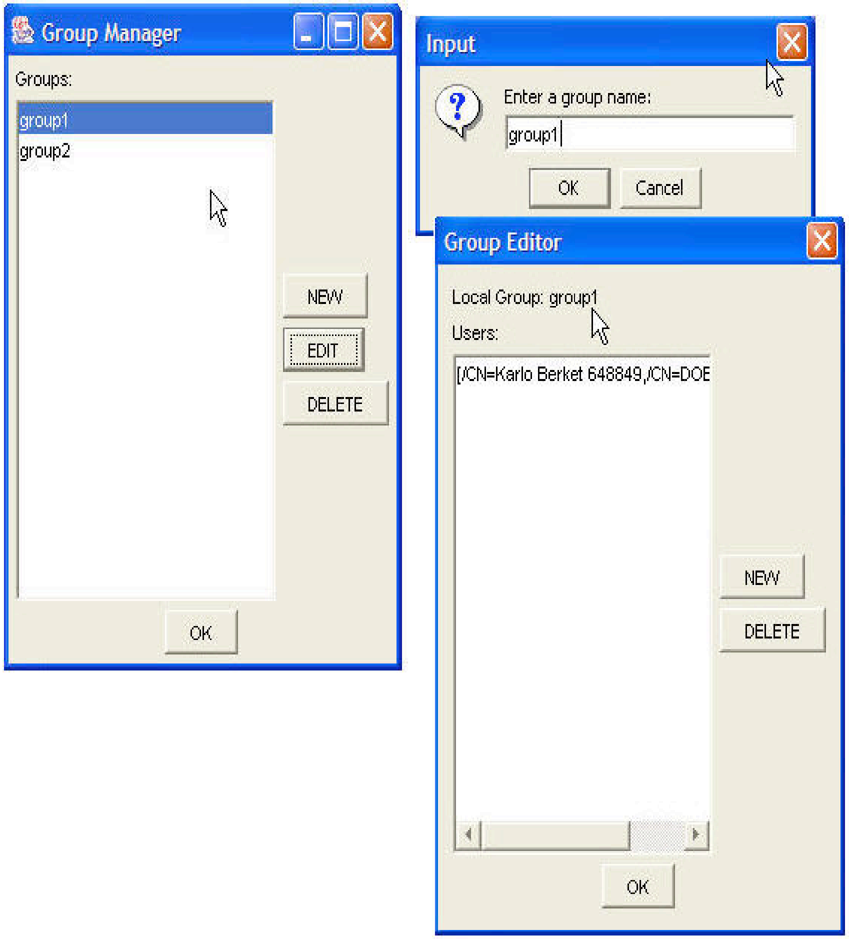
Groups:

group2

Rejected Users:

ratas 208666,/CN=DOEGrids CA 1]

Manage Groups



Groups:

group1
group2

Enter a group name:

group1

Local Group: group1

Users:

[/CN=Karlo Berket 648849,/CN=DOE

On-going Work

- Performance measurements (security impact, scalability, etc.)
- Remote groups
- Securing the queries
- Providing access control to search group

More Information

- Project page: http://www.dsd.lbl.gov/P2P/file-share
- Software download: http://www.dsd.lbl.gov/scishare
- E-mail: kberket@lbl.gov